

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
6 November 2003 (06.11.2003)

PCT

(10) International Publication Number  
**WO 03/092190 A1**

(51) International Patent Classification<sup>7</sup>: **H04B 7/26**

(21) International Application Number: PCT/KR02/01987

(22) International Filing Date: 24 October 2002 (24.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
2002-0022346 23 April 2002 (23.04.2002) KR

(71) Applicant (for all designated States except US): **SK TELECOM CO., LTD** [KR/KR]; 99, Seorin-dong, Jong-gro-gu, Seoul 110-110 (KR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **SHIN, Yong-Sik** [KR/KR]; 9-1 SK Telecom Network Research, Sunae-dong, Bundang-gu, Seongnam-si, Gyeonggi-do 463-784 (KR). **RYU, Si-Hoon** [KR/KR]; 9-1 SK Telecom Network Research, Sunae-dong, Bundang-gu, Seongnam-si, Gyeonggi-do 463-784 (KR). **LEE, Dong-Hahk** [KR/KR]; 9-1 SK Telecom Network Research, Sunae-dong, Bundang-gu, Seongnam-si, Gyeonggi-do

463-784 (KR). **BHANG, Chan-Jeom** [KR/KR]; 9-1 SK Telecom Network Research, Sunae-dong, Bundang-gu, Seongnam-si, Gyeonggi-do 463-784 (KR).

(74) Agents: **KIM, Seong-Nam** et al.; 17th Floor, City Air Tower, 159-9 Samsung-dong, Gangnam-gu, Seoul 135-973 (KR).

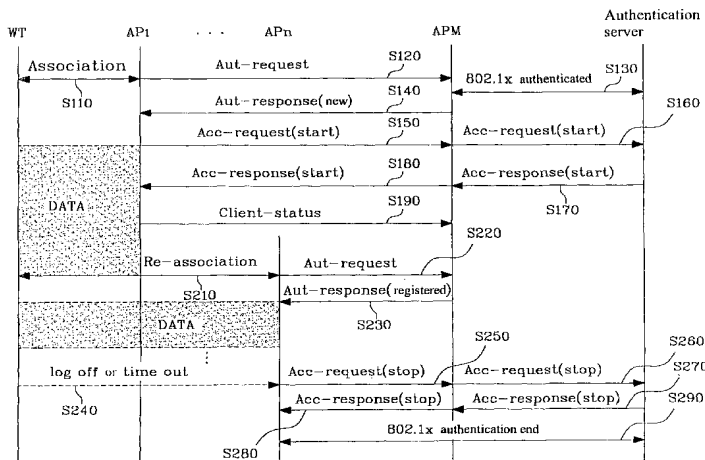
(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:  
— with international search report

[Continued on next page]

(54) Title: AUTHENTICATION SYSTEM AND METHOD HAVING MOBILITY IN PUBLIC WIRELESS LOCAL AREA NETWORK



(57) Abstract: The present invention discloses an authentication system and method having mobility in a public wireless LAN. The authentication system includes an access point for requesting authentication of a wireless terminal to an access point manager, enabling data transmission and reception of the authenticated wireless terminal, and requesting the access point manager to charge the wireless terminal, and the access point manager for authenticating the wireless terminal which has already been authenticated on the basis of previously-registered registration information upon the request of the access point, authenticating the wireless terminal which has not been registered through an authentication server of a wireless network operator, and transmitting the authentication information to the access point. As a result, the wireless terminal can continuously access the network through the access points of the same subnet as well as different subnet without re-authentication, thereby achieving mobility and processing charging.



WO 03/092190 A1



---

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

# **AUTHENTICATION SYSTEM AND METHOD HAVING MOBILITY IN PUBLIC WIRELESS LOCAL AREA NETWORK**

## **5 Technical Field**

The present invention relates to authentication of a wireless terminal, and in particular to an authentication system and method having mobility in a public wireless local area network (LAN) which allow a wireless terminal to access an access point of one  
10 subnet and receive authentication, and validate authentication and charging even if the wireless terminal moves to an access point of a different subnet.

## **Background Art**

15 The 802.11b standard leading a generally-used public wireless LAN does not cover authentication. To authenticate users, the 801.1x has been used. That is, the wireless LAN does not support wide mobility.

In order for a wireless terminal using the wireless LAN to roam between access points, the access points must be added with a roaming function. For this, standardization  
20 processes have been performed under the IEEE 802.11f. Some companies support the wireless terminal to roam between the access points by adding an intrinsic function. Here, roaming implies movement between the access points positioned in the identical subnet.

Fig. 1 is a schematic view illustrating a conventional LAN system of a wireless network operator. Reference numeral 10 denotes a network, WT denotes a wireless  
25 terminal, 20 denotes an access point, 30 denotes an IP network core, 40 denotes a wireless

network, 42 denotes an authentication server, 44 denotes a wireless network operator core, 46 denotes a mobile switching center/home location register (MSC/HLR) and 48 denotes a charging gateway.

The conventional LAN system of the wireless network operator transmits a control signal data to the wireless network operator core 44. The access point 20 routes a user data packet directly to the IP network core 30 to access a public or personal service.

Referring to Fig. 1, the wireless terminal accesses the access point 20 and receives an IP address from the access point 20. The access point 20 transmits an authentication request to the authentication server 42 composing a gateway between an access network and a signal network. The authentication server 42 queries the HLR 46 about the authentication data, and authenticates the user according to the authentication data.

Fig. 2 is a detailed view illustrating an authentication process by the conventional public wireless LAN and the wireless network operator system of Fig. 1.

As shown in Fig. 2, the wireless terminal WT accesses the network 10 through the access point 20 (S11). Thereafter, the wireless terminal WT receives the IP address from the access point 20 and transmits an initial authentication request to the access point 20. The authentication server 42 accesses the MSC/HLR 46 and requests a triplet to the HLR. Then, the authentication server 42 transmits random number authentication (RAND) to the wireless terminal WT through the access point 20 according to a message authentication code calculated by the RAND (S21).

The message authentication code achieves mutual authentication between the wireless network 40 and the wireless terminal WT. The wireless terminal WT calculates a message authentication code and compares the result with the message authentication code from the network 10 (S23).

When the wireless terminal WT transmits the calculated message authentication

code to the access point 20, the access point 20 transmits the response to the authentication server 42 (S27 and S29). The authentication server 42 calculates a message authentication code and verifies the response of the wireless terminal WT (S31). Thereafter, the authentication server 42 transmits an authentication result code to the access point (S33).

5 Here, when the authentication is successful, the access point 20 notifies initiation of a new account session to the authentication server 42 (S35).

Finally, the access point 20 routes a terminal data packet and transmits an acknowledgement signal to the wireless terminal WT (S37).

However, the conventional method always requests re-authentication for roaming.  
10 That is, when the wireless terminal moves to a new access point area, the wireless terminal must be authenticated by the new access point. Such re-authentication does not guarantee continuity of data. In addition, the related methods do not include a charging process and thus not satisfy the operators.

## 15 **Disclosure of Invention**

Accordingly, it is an object of the present invention to provide an authentication system and method having mobility in a public wireless LAN which guarantee mobility of a wireless terminal by authenticating the wireless terminal on the basis of the previously-  
20 authenticated registration information, even if the wireless terminal authenticated by one access point moves to another access point of a different subnet.

In order to achieve the above-described object of the invention, there is provided an authentication system having mobility in a public wireless LAN which processes authentication and charging through an authentication server of a wireless network  
25 operator, including: an access point wirelessly connected to a wireless terminal, for

outputting an authentication request message or charging request message added with information of the wireless terminal and requesting authentication and charging of the wireless terminal, and receiving an authentication response message and enabling data transmission and reception of the authenticated wireless terminal; and an access point  
5 manager for receiving the authentication request message for the wireless terminal from the access point, confirming whether the wireless terminal has already been authenticated, transmitting the authentication request message to the authentication server of the wireless network operator and transmitting the received authentication response message to the access point when the wireless terminal has not been authenticated, and transmitting the  
10 authentication response message to the access point on the basis of the registered authentication information when the wireless terminal has been authenticated.

According to another aspect of the invention, an authentication method having mobility in a public wireless LAN which receives an authentication or charging request message for a wireless terminal from an access point and processes authentication and  
15 charging through an authentication server of a wireless network operator includes: an authentication step for receiving the authentication request message from the access point, authenticating the wireless terminal on the basis of the authentication request message, and transmitting an authentication response message to the corresponding access point; and a charging step for receiving the charging request message from the access point and  
20 transmitting the received charging request message to the authentication server, and receiving a charging request response message from the authentication server and transmitting the received charging request response message to the access point.

According to another aspect of the invention, an authentication method having mobility in a public wireless LAN where an access point requests authentication and  
25 charging of a wireless terminal through an access point manager includes: a step for the

access point to be wirelessly connected to the wireless terminal; an authentication request step for adding information of the wireless terminal to an authentication request message and transmitting it to the access point manager; and a step for receiving an authentication response message to the authentication request message transmitted in the authentication request step from the access point manager, and selectively requesting the access point manager to start charging on the basis of the authentication information included in the authentication response message.

### **Brief Description of the Drawings**

10

The present invention will become better understood with reference to the accompanying drawings which are given only by way of illustration and thus are not limitative of the present invention, wherein:

Fig. 1 is a schematic view illustrating an access state of a conventional public wireless LAN and wireless network operator system;

Fig. 2 is a detailed view illustrating an authentication process by the conventional public wireless LAN and wireless network operator system of Fig. 1;

Fig. 3 is a structure view illustrating an authentication and charging system by a public wireless LAN and wireless network operator system in accordance with a preferred embodiment of the present invention;

Fig. 4 shows a protocol for processing authentication and charging among a wireless terminal, an access point, an access point manager and an authentication server of Fig. 3;

Fig. 5 shows formats of an authentication request message, an authentication response message and a wireless terminal status message of Fig. 4;

Fig. 6 is a detailed flowchart showing the operation of the access point of Fig. 4;  
and

Fig. 7 is a detailed flowchart showing the operation of the access point manager of Fig. 4.

5

### **Best mode for Carrying Out the Invention**

An authentication system and method having mobility in a public wireless LAN in accordance with a preferred embodiment of the present invention will now be described  
10 in detail with reference to Figs. 3 to 7.

Fig. 3 is a structure view illustrating the authentication system by the public wireless LAN and wireless network operator system in accordance with the preferred embodiment of the present invention. Reference numerals 120 and 140 denote access points, 130 denotes an IP network core, 160 denotes an access point manager(APM), 310  
15 denotes an authentication server, 320 denotes an MSC/HLR, 330 denotes a wireless network operator core, and 340 denotes a charging gateway. In addition, WT denotes a wireless terminal, MSC is a mobile switching center and HLR is a home location register.

As depicted in Fig. 3, a plurality of access points 120 and 140 access the IP network core 130. Each of the access points 120 and 140 composes a subnet for wirelessly  
20 accessing the plurality of wireless terminals WT to the IP network core 130. A necessary number of access points can access the IP network core 130 according to the structure of the operator.

The access point manager 160 access the IP network core 130 to manage authentication and charging of the whole access points 120 and 140 accessing the IP  
25 network core 130. In addition, the access point manager 160 accesses the authentication



server 310 of the wireless network operator.

Still referring to Fig. 3, reference 300 denotes an area of the wireless network operator. The authentication server 310, the MSC/HLR 320 and the charging gateway 340 access the wireless network operator core 330.

5 Accordingly, the access point manager 160 requests authentication and charging through the authentication server 310 of the wireless network operator. When receiving an authentication request from the access point manager 160, the authentication server 310 accessing the wireless network operator core 330 processes the authentication request through the MSC/HLR 320, and when receiving a charging request, the authentication  
10 server 310 processes the charging request through the charging gateway 340. Thereafter, the authentication server 310 transmits the authentication request or charging request result to the access point manager 160.

Fig. 4 shows a protocol for processing authentication and charging among the wireless terminal WT, the access point AP, the access point manager APM and the  
15 authentication server 310 of Fig. 3. Reference numeral WT denotes the wireless terminal, AP1 denotes the first access point 120, APn denotes the nth access point 140, and APM denotes the access point manager 160.

Fig. 4 shows a message transmission process until the wireless terminal WT associated with the first access point AP1 of the first access point area 110 accesses the nth  
20 access point 140 of the nth access point area 150 and ends access to the nth access point 140.

The wireless terminal WT is associated with the first access point AP1. Here, the first access point AP1 transmits an authentication request message Aut-request to the access point manager APM (S120). The authentication request message Aut-request  
25 includes user ID and password information. In addition, the authentication request message

Aut-request includes the IP address of the access point AP1 currently transmitting the authentication request message.

The access point manager APM authenticates the wireless terminal WT through the authentication server 310 upon the authentication request of the first access point AP1 (S130). The authentication between the access point manager APM and the authentication server 310 can be processed by selectively using for example, MD-5, TLS, SRP and OTP. Accordingly, the wireless terminal is authenticated. The access point manager APM transmits an authentication response message Aut-response to the corresponding access point AP1 (S140). Here, the authentication response message Aut-response includes authentication registration information.

When authentication of the wireless terminal WT is finished, the first access point AP1 enables data transmission and reception of the wireless terminal WT, and transmits a charging start request message Acc-request(start) to the access point manager APM (S150). The access point manager APM transmits the charging start request message Acc-request(start) received from the first access point AP1 to the authentication server 310 to start charging (S160).

When the access point manager APM receives a charging start response message Acc-response(start) from the authentication server 310 (S170), it transmits the charging start response message Acc-response(start) to the first access point AP1. The first access point AP1 transmits information of the authenticated wireless terminal to the access point manager APM through a wireless terminal status message Wireless terminal-status (S190).

Accordingly, the first authentication and charging are started due to association between the wireless terminal WT and the first access point AP1. The process where the wireless terminal WT is associated with the nth access point APn and completes authentication will now be explained in detail.

When the wireless terminal WT moves to the nth access point APn, the wireless terminal WT is re-associated with the nth access point APn (S210). The nth access point APn transmits the authentication request message Aut-request to the access point manager APM (S220). The access point manager APM receiving the authentication request message Aut-request extracts the information of the wireless terminal WT included in the authentication request message Aut-request, and confirms whether the wireless terminal WT has already been authenticated. Since the wireless terminal WT has been authenticated, the access point manager APM does not request authentication to the authentication server 301 but transmits the authentication response message Aut-response to the nth access point APn for authentication (S230). The access point manager APM authenticates the wireless terminal WT when a MAC address and an allocated IP address of the wireless terminal WT included in the received authentication request message Aut-request are identical to a MAC address and an allocated IP address of the wireless terminal WT stored in a management table and when an IP address of the access point is changed.

When receiving the authentication response message Aut-response from the access point manager APM (S230), the nth access point APn enables data transmission and reception of the wireless terminal WT.

When the nth access point APn receives a log off request from the wireless terminal WT during the data transmission or time-out is generated due to interruption of the data transmission (S240), the nth access point APn transmits a charging stop request message Acc-request(stop) to the access point manager APM to stop charging (S250).

The access point manager APM transmits the charging stop request message Acc-request(stop) received from the nth access point APn to the authentication server 310 (S260). Thereafter, when receiving a charging stop response message Acc-response(stop) from the authentication server 310 (S270), the access point manager APM transmits it to

the nth access point APn (S280). Therefore, the authentication between the nth access point APn and the authentication server 310 is finished (S290).

Fig. 5 shows formats of the authentication request message, the authentication response message and the wireless terminal status message of Fig. 4.

5 Fig. 5a shows a format of the authentication request message.

Here, ISAMP version is a field representing a version of an inter subnet-access point mobile protocol which implies a protocol of the invention, and is composed of for example 1 byte. Identifier is a field representing a message identifier and is composed of for example 2 bytes. Length is a field representing a length of IARP packet and is composed of for example 2 bytes. AP-IP address is a field representing an address of the current access point. Wireless terminal-MAC address includes an address length defined as a field representing a media access control(MAC) address of the currently-associated wireless terminal. User ID is a field representing identification of the user. Sequence Number is a field representing a serial number and is composed of 2 bytes. For instance,  
15 Sequential Number has a value from 0 to 2048.

Fig. 5b shows a format of the authentication response message.

Here, ISAMP version is a field representing a version of an inter subnet-access point mobile protocol and is composed of for example 1 byte. Identifier is a field representing a message identifier and is composed of for example 2 bytes. Length is a field representing a length of IARP packet and is composed of for example 2 bytes. AP-IP  
20 address is a field representing an address of the current access point. Connection is a field representing identification of authentication registration and is composed of for example 1 byte. Connection respectively displays a state where the wireless terminal firstly requests authentication and a state where the wireless terminal which has already been authenticated  
25 and registered requests authentication. For instance, Connection is set up as 00h for the

newly-registered wireless terminal and 11h for the previously-registered wireless terminal. Sequence Number is a field representing a serial number and is composed of 2 bytes. For example, Sequential Number has a value from 0 to 2048.

Fig. 5c shows a format of the wireless terminal status message.

5 Here, ISAMP version is a field representing a version of an inter subnet-access point mobile protocol and is composed of for example 1 byte. Identifier is a field representing a message identifier and is composed of for example 2 bytes. Length is a field representing a length of IARP packet and is composed of for example 2 bytes. AP-IP address is a field representing an address of the current access point. Wireless terminal-  
10 MAC address includes an address length defined as a field representing a media access control address of the currently-associated wireless terminal. Wireless terminal-IP address is a field representing an IP address allocated to the wireless terminal. Sequence Number is a field representing a serial number and is composed of 2 bytes. For instance, Sequential Number has a value from 0 to 2048.

15 Fig. 6 is a detailed flowchart showing the operation of the access point AP of Fig. 4.

The access point AP is associated with the wireless terminal WT in each area (S310). Then, the access point AP provides the wireless terminal information and the access point information to the access point manager APM to request authentication (S320).  
20 Here, the access point AP transmits the information to the access point manager APM through the authentication request message Aut-request.

The access point AP confirms whether the access point manager APM responds to the authentication request (S330). Here, the access point AP receives the authentication information from the access point manager APM through the authentication response  
25 message Aut-response.

When the authentication is normally finished, the access point AP analyzes the received authentication response message, and confirms whether the wireless terminal WT has already been registered or is newly registered (S340). For example, when the value of Connection field of the authentication response message Aut-response is 00h, the access point AP decides that the wireless terminal is newly registered, and when the value of Connection field is 11h, the access point AP decides that the wireless terminal has already been registered.

When the wireless terminal is newly registered (00h), the access point AP requests the access point manager APM to start charging (S350). Here, the access point AP transmits information through the charging start request message Acc-request(start). In addition, the access point AP enables data transmission and reception of the wireless terminal WT (S360). When receiving the charging start request response from the access point manager APM (S370), the access point AP transmits the wireless terminal status information to the access point manager APM (S380). The wireless terminal status information is transmitted from the access point AP to the access point manager APM through the wireless terminal status message Wireless terminal-status.

On the other hand, when the access point AP confirms that the wireless terminal WT has already been registered by analyzing the authentication response message Aut-response(11h), the access point AP does not request the access point manager APM to start charging but continuously enables data transmission and reception of the wireless terminal (S385).

In addition, the access point AP confirms whether the log off request is received from the wireless terminal WT or time-out is generated (S390). If so, the access point AP requests the access point manager APM to stop charging (S400). Here, the access point AP transmits the information through the charging stop request message Acc-request(stop).

The access point AP receives the charging stop request response message from the access point manager APM (S410). Accordingly, the authentication of the wireless terminal WT between the access point AP and the authentication server 310 is finished(S420).

Fig. 7 is a detailed flowchart showing the operation of the access point manager  
5 APM of Fig. 4.

The access point manager APM confirms whether the authentication request is received from the access point AP (S510). Here, the access point manager APM receives the authentication request message Aut-request from the access point AP. When receiving the authentication request message Aut-request from the access point AP, the access point  
10 manager APM confirms whether the wireless terminal WT has been authenticated by analyzing the authentication request message Aut-request (S610). That is, the access point manager APM confirms whether the wireless terminal WT has been authenticated by referring to the MAC address and IP address of the wireless terminal WT and the IP address of the access point AP included in the received authentication request message  
15 Aut-request.

In the case that the wireless terminal WT has not been authenticated, the access point manager APM transmits the authentication request message Aut-request to the authentication server 310 to request authentication (S620). Thereafter, the access point manager APM receives the authentication information from the authentication server 310  
20 (S630). When the authentication is normally processed, the access point manager APM stores the wireless terminal information, access point information and authentication information (S640). The access point manager APM transmits the authentication response message Aut-response to the access point AP which requests authentication (S650). Here, the access point manager APM sets up Connection field of the authentication response  
25 message Aut-response as for example, 00h, thereby notifying that the wireless terminal

WT is newly authenticated.

When the wireless terminal WT has been authenticated, the access point manager APM does not request authentication to the authentication server 310 but directly authenticates the wireless terminal WT. Here, the access point manager APM renews and stores the IP address of the access point AP included in the authentication request message Aut-request (S660). Thereafter, the access point manager APM transmits the authentication response message Aut-response to the access point AP which requests authentication (S670). Here, the access point manager APM sets up Connection field of the authentication response message Aut-response as for example, 11h, thereby notifying that the wireless terminal WT has already been authenticated.

On the other hand, the access point manager APM confirms whether the charging request signal is received from the access point AP (S520). When receiving the charging start request message Acc-request(start) from the access point AP, the access point manager APM transmits the charging start request message Acc-request(start) to the authentication server 310 to request charging (S530). Thereafter, when receiving the charging start response message Acc-response(start) from the authentication server 310, the access point manager APM transmits the charging start response message Acc-response(start) to the corresponding access point AP (S550). In addition, the access point manager APM receives the wireless terminal status message Wireless terminal-status showing the status of the wireless terminal WT from the access point AP (S560).

When receiving the charging stop request message Acc-request(stop) from the access point AP, the access point manager APM transmits the received charging stop request message Acc-request(stop) to the authentication server 310 to stop charging (S570). Then, when receiving the charging stop response message Acc-response(stop) from the authentication server 310, the access point manager APM transmits the charging stop



response message Acc-response(stop) to the corresponding the access point AP (S590).  
Therefore, the authentication of the wireless terminal WT between the access point AP and the authentication server 310 is finished (S600).

As the present invention may be embodied in several forms without departing  
5 from the spirit or essential characteristics thereof, it should also be understood that the  
above-described embodiment is not limited by any of the details of the foregoing  
description, unless otherwise specified, but rather should be construed broadly within its  
spirit and scope as defined in the appended claims, and therefore all changes and  
modifications that fall within the metes and bounds of the claims, or equivalences of such  
10 metes and bounds are therefore intended to be embraced by the appended claims.

As discussed earlier, in accordance with the present invention, when the wireless  
terminal moves between the access points of the same subnet as well as different subnet,  
the access point manager manages the previously-authenticated information and  
authenticates the wireless terminal in the access point. As a result, the wireless terminal  
15 can continuously access the network without re-authentication, thereby achieving mobility  
and processing charging.

**What is claimed is:**

1. An authentication system having mobility in a public wireless LAN which processes authentication and charging through an authentication server of a wireless network operator, comprising:

an access point wirelessly connected to a wireless terminal, for outputting an authentication request message or charging request message added with information of the wireless terminal and requesting authentication and charging of the wireless terminal, and receiving an authentication response message and controlling data transmission and reception of the authenticated wireless terminal; and

an access point manager for receiving the authentication request message for the wireless terminal from the access point, confirming whether the wireless terminal has already been authenticated, transmitting the authentication request message to the authentication server of the wireless network operator and transmitting the received authentication response message to the access point when the wireless terminal has not been authenticated, and transmitting the authentication response message to the access point on the basis of the registered authentication information when the wireless terminal has been authenticated.

2. The system according to claim 1, wherein the access point adds a MAC address and IP address of the wireless terminal which needs authentication to the authentication request message and transmits the resultant message.

3. The system according to claim 1, wherein the access point adds an IP address of the access point which requests authentication to the authentication request message and transmits the resultant message.

4. The system according to claim 1, wherein the access point adds a user ID

and password from the wireless terminal which needs authentication to the authentication request message and transmits the resultant message.

5        5.        The system according to claim 1, wherein the access point confirms whether the wireless terminal is newly authenticated or has already been authenticated on the basis of the authentication information included in the authentication response message.

6.        The system according to claim 1, wherein, when the access point confirms that the wireless terminal is newly authenticated on the basis of the authentication information included in the authentication response message, the access point transmits a charging start request message to the access point manager to start charging the  
10        authenticated wireless terminal.

7.        The system according to claim 1, wherein, when the access point transmits the charging start request message to start charging the authenticated wireless terminal, the access point controls data transmission and reception of the authenticated wireless terminal.

15        8.        The system according to claim 1, wherein the access point transmits status information of the wireless terminal to the access point manager after transmitting the charging start request message.

9.        The system according to claim 1, wherein, when a logoff request is received from the wireless terminal or time-out is generated, the access point transmits a  
20        charging stop request message to the access point manager to stop charging.

10.       The system according to claim 1, wherein, when the access point manager receives the authentication request message from the access point, the access point manager confirms whether the wireless terminal has already been authenticated.

11.       The system according to claim 1, wherein, when the access point  
25        manager confirms that the wireless terminal has not been authenticated on the basis of the

authentication request message, the access point manager transmits the authentication request message to the authentication server of the wireless network operator for authentication.

12. The system according to claim 1, wherein, when the access point  
5 manager confirms that the wireless terminal is newly authenticated, the access point manager adds new authentication information to the authentication response message, and transmits the resultant message to the access point.

13. The system according to claim 1, wherein, when the access point  
manager confirms that the wireless terminal has already been authenticated on the basis of  
10 the authentication request message, the access point manager directly authenticates the wireless terminal on the basis of the registered authentication information.

14. The system according to claim 1, wherein, when the wireless terminal  
has already been authenticated, the access point manager adds previous authentication  
information to the authentication response message, and transmits the resultant message to  
15 the access point.

15. The system according to claim 1, wherein, when the access point  
manager receives a charging start request message for the wireless terminal from the access  
point, the access point manager transmits the charging start request message to the  
authentication server to start charging.

20 16. The system according to claim 1, wherein, when the access point  
manager receives a charging stop request message for the wireless terminal from the access  
point, the access point manager transmits the charging stop request message to the  
authentication server to stop charging.

17. An authentication method having mobility in a public wireless LAN  
25 which receives an authentication or charging request message for a wireless terminal from

an access point and processes authentication and charging through an authentication server of a wireless network operator, comprising:

an authentication step for receiving the authentication request message from the access point, authenticating the wireless terminal on the basis of the authentication request message, and transmitting an authentication response message to the corresponding access point; and

a charging step for receiving the charging request message from the access point and transmitting the received charging request message to the authentication server, and receiving a charging request response message from the authentication server and transmitting the received charging request response message to the access point.

18. The method according to claim 17, wherein the authentication step comprises the steps of:

deciding whether the wireless terminal has already been authenticated on the basis of the authentication request message received from the access point;

transmitting the authentication response message to the access point on the basis of the previously-registered authentication information, when the wireless terminal has already been authenticated; and

obtaining authentication from the authentication server and transmitting the authentication response message to the access point, when the wireless terminal has not been authenticated.

19. The method according to claim 18, wherein the step for obtaining authentication from the authentication server and transmitting the authentication response message to the access point comprises a step for registering wireless terminal information, access point information and authentication information.

20. The method according to claim 18, wherein the step for transmitting the

authentication response message to the access point on the basis of the previously-registered authentication information comprises a step for renewing the access point information on the basis of the received authentication request message.

21. The method according to claim 18, wherein the step for transmitting the authentication response message comprises a step for adding information on whether the wireless terminal is newly authenticated or has already been authenticated to the authentication response message.

22. An authentication method having mobility in a public wireless LAN where an access point requests authentication and charging of a wireless terminal through an access point manager, comprising:

a step for the access point to be wirelessly connected to the wireless terminal;

an authentication request step for adding information of the wireless terminal to an authentication request message and transmitting it to the access point manager; and

a step for receiving an authentication response message to the authentication request message transmitted in the authentication request step from the access point manager, and selectively requesting the access point manager to start charging on the basis of the authentication information included in the authentication response message.

23. The method according to claim 22, wherein the step for requesting authentication comprises a step for adding a MAC address and IP address of the wireless terminal to the authentication request message.

24. The method according to claim 22, wherein the step for requesting authentication comprises a step for adding an IP address of the access point to the authentication request message.

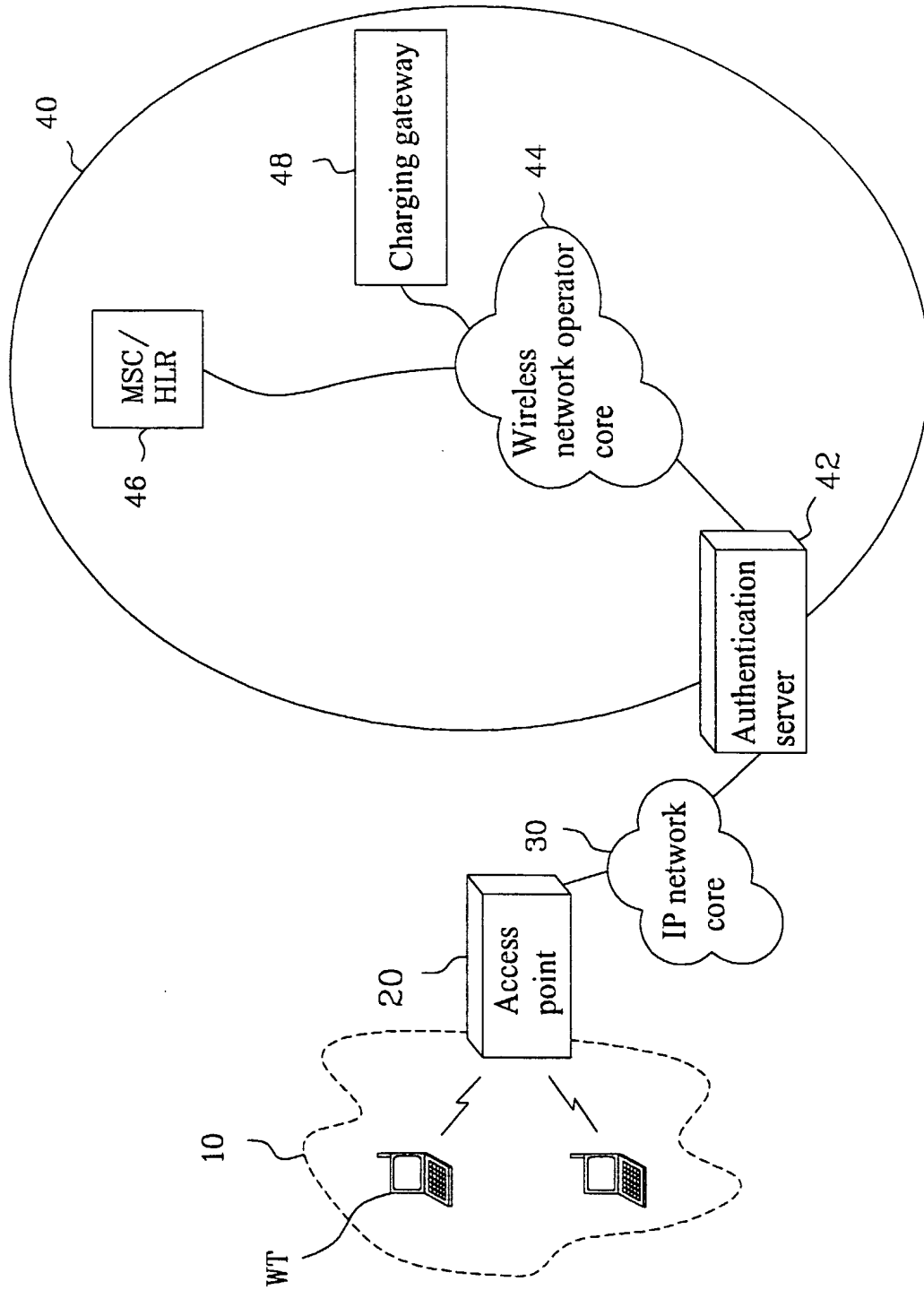
25. The method according to claim 22, wherein the step for requesting the access point manager to start charging comprises the steps of:

deciding whether the wireless terminal is newly authenticated on the basis of the received authentication response message;

transmitting a charging start request message to the access point manager to start charging and starting data transmission and reception of the wireless terminal, when the  
5 wireless terminal is newly authenticated; and

starting data transmission and reception of the wireless terminal when the wireless terminal has already been authenticated.

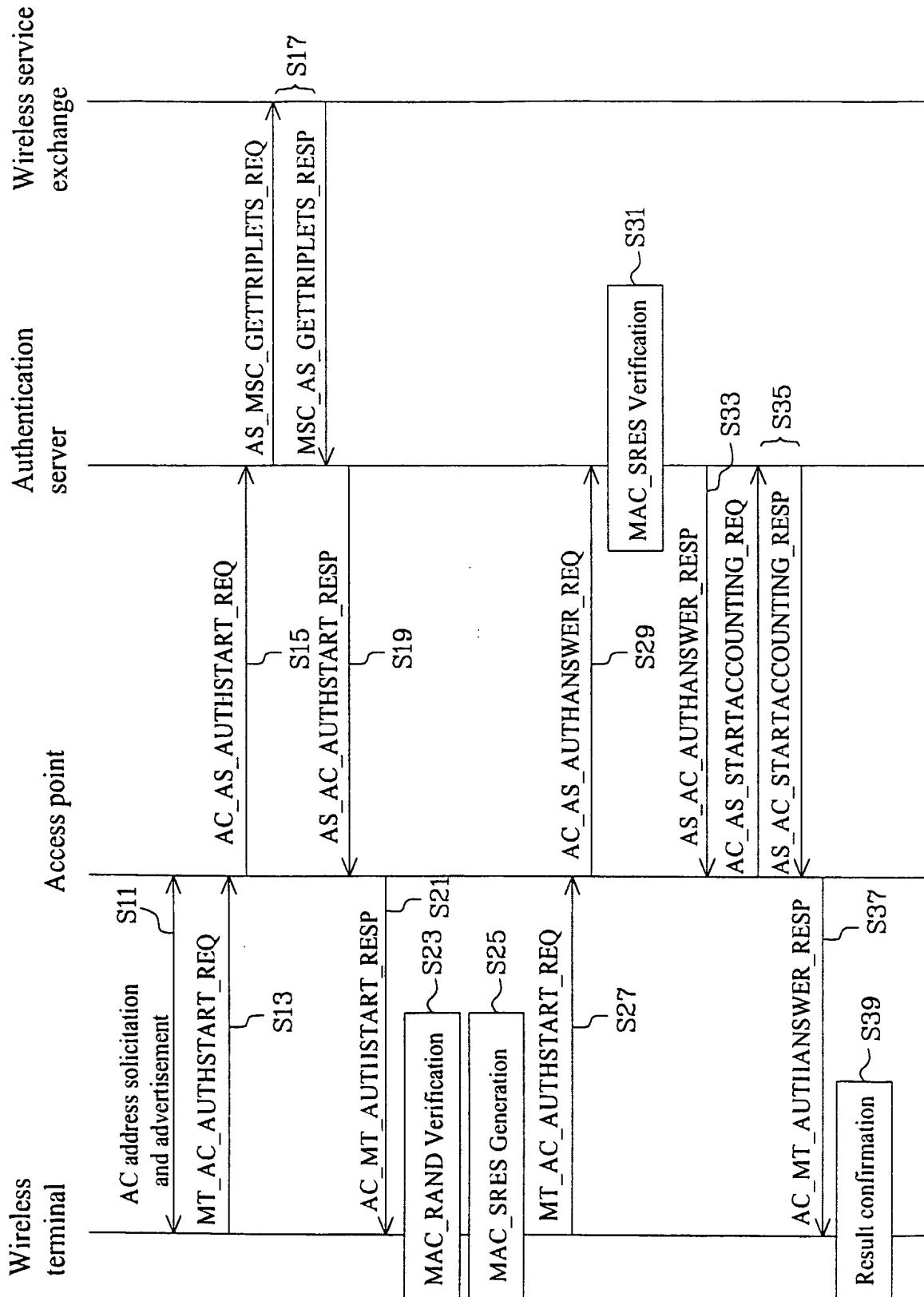
1/9  
FIG. 1





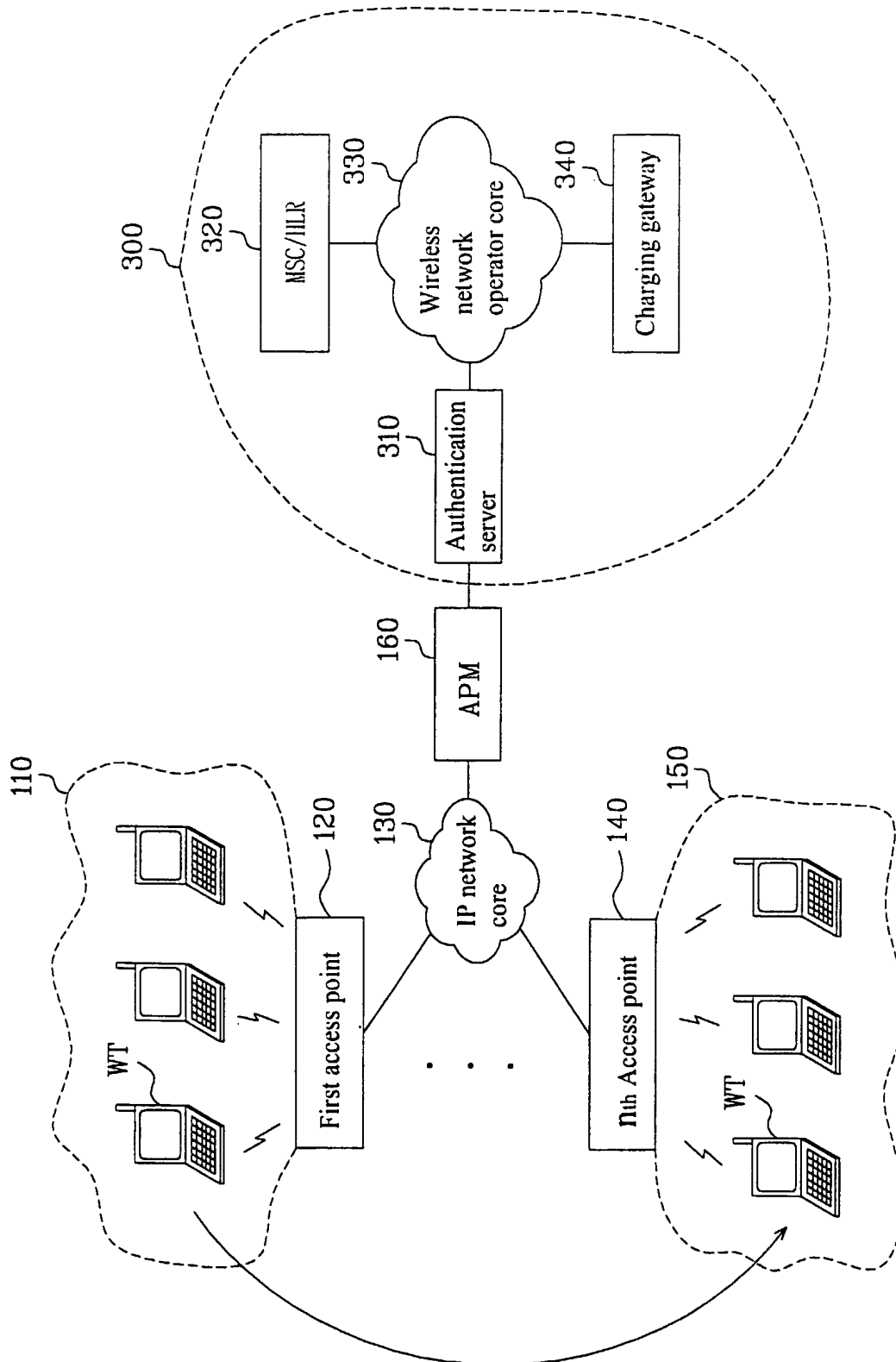
2/9

FIG. 2



3/9

FIG. 3



4/9

FIG. 4

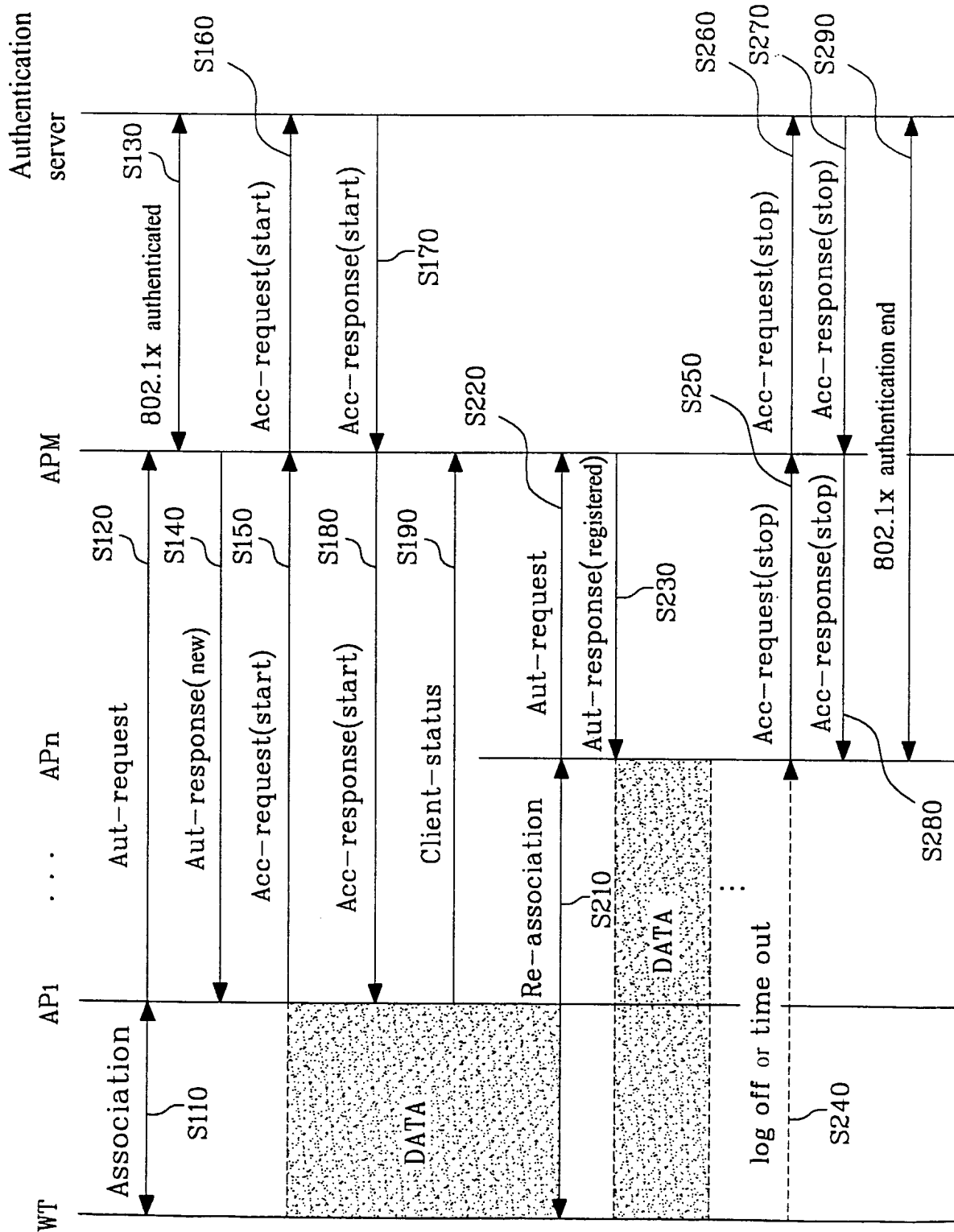


FIG. 5A

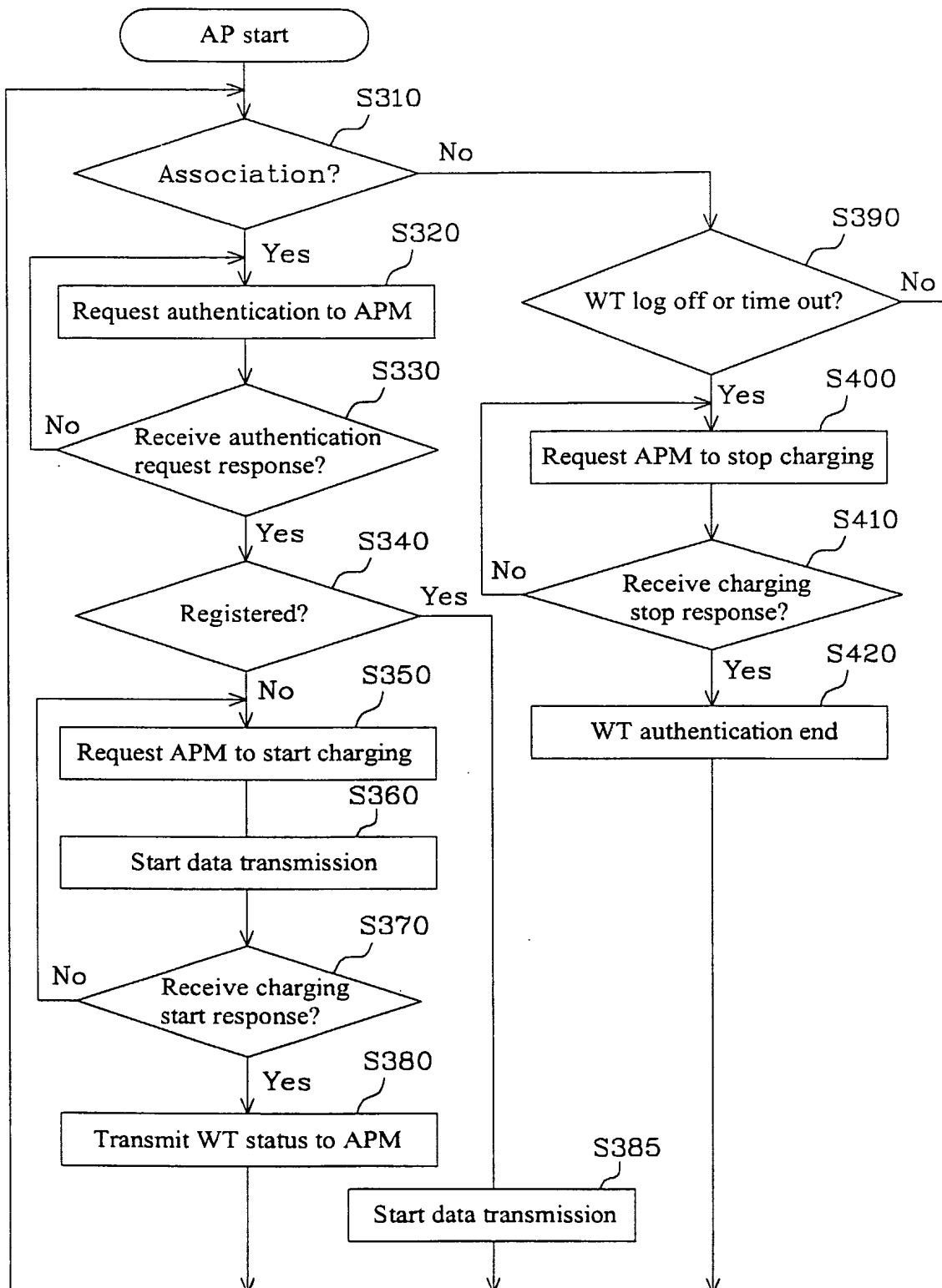
ISAMP version	Identifier	Length	AP-IP address	Client-MAC address	User ID	User password	Sequence Number	Others	
------------------	------------	--------	------------------	-----------------------	---------	------------------	--------------------	--------	--

6/9  
FIG. 5B

ISAMP version	Identifier	Length	AP-IP address	Connection	Sequence Number	Others	
------------------	------------	--------	------------------	------------	--------------------	--------	--

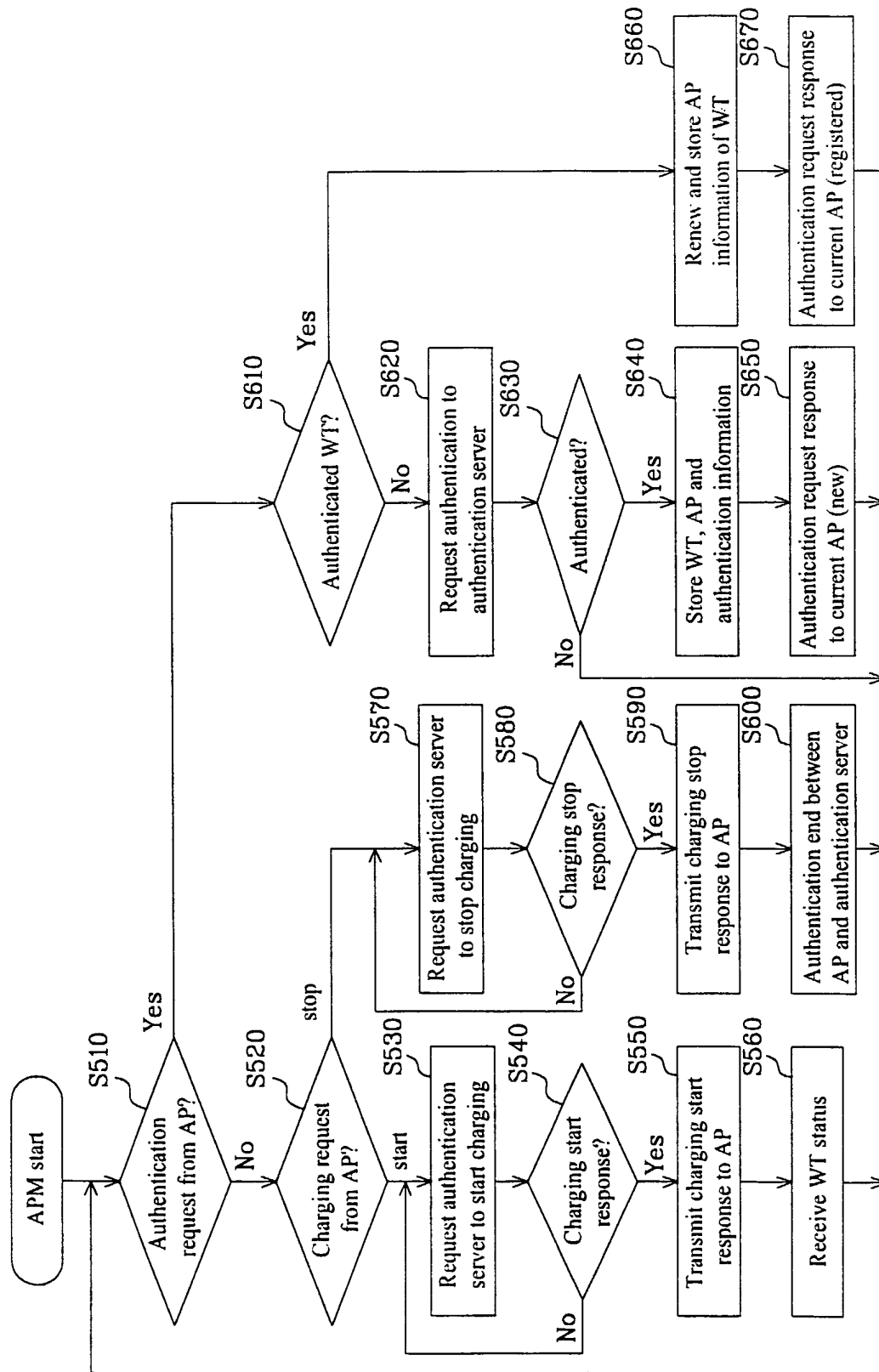
FIG. 5C

ISAMP version	Identifier	Length	AP-IP address	Client-MAC address	Client-IP address	Sequence Number	Others	
------------------	------------	--------	------------------	-----------------------	----------------------	--------------------	--------	--

8/9  
FIG. 6

9/9

FIG. 7





# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/KR02/01987

## A. CLASSIFICATION OF SUBJECT MATTER

**IPC7 H04B 7/26**

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L, H04B, H04Q, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Patents and applications for inventions since 1975, Korean Utility models and applications for Utility models since 1975, IEEE technical document since 1980

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 2002-0023917 A (iMnetpia.co.ltd) 20020329 See the whole document	1, 17, 22
Y	KR 2001-0090038 A (daesung digital tech co. ltd) 20011018 See the whole document	1, 17, 22
A	EP 851633 A2 (Lucent tech) 19991110 See the whole document	1-25
A	EP 1161031 A2 (Sharp) 2001120 See abstract	1-25
A	JP 13345819 A (Sharp) 20011214 See abstract	1-25
P. A	KR 2002-0035530 A (TG infonet. co. ltd) 20020511 See the whole document	1-25

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

\* Special categories of cited documents:


"A" document defining the general state of the art which is not considered to be of particular relevance  
 "E" earlier application or patent but published on or after the international filing date  
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)  
 "O" document referring to an oral disclosure, use, exhibition or other means  
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
 "&" document member of the same patent family

Date of the actual completion of the international search  
10 FEBRUARY 2003 (10.02.2003)

Date of mailing of the international search report  
17 FEBRUARY 2003 (17.02.2003)

Name and mailing address of the ISA/KR

 Korean Intellectual Property Office  
920 Dunsan-dong, Seo-gu, Daejeon 302-701,  
Republic of Korea  
Facsimile No. 82-42-472-7140

Authorized officer

KIM, Yong Jae  
Telephone No. 82-42-481-5716



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR02/01987

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 851633 A2	19991110	CA 2221948 AA JP 10210533 A2	19980630 19980807

**PUB-NO:** WO003092190A1  
**DOCUMENT-IDENTIFIER:** WO 3092190 A1  
**TITLE:** AUTHENTICATION SYSTEM AND  
METHOD HAVING MOBILITY IN  
PUBLIC WIRELESS LOCAL AREA  
NETWORK  
**PUBN-DATE:** November 6, 2003

**INVENTOR-INFORMATION:**

<b>NAME</b>	<b>COUNTRY</b>
SHIN, YONG-SIK	KR
RYU, SI-HOON	KR
LEE, DONG-HAHK	KR
BHANG, CHAN-JEOM	KR

**ASSIGNEE-INFORMATION:**

<b>NAME</b>	<b>COUNTRY</b>
SK TELECOM CO LTD	KR
SHIN YONG-SIK	KR
RYU SI-HOON	KR
LEE DONG-HAHK	KR
BHANG CHAN-JEOM	KR

**APPL-NO:** KR00201987  
**APPL-DATE:** October 24, 2002

**PRIORITY-DATA:** KR2002022346A (April 23, 2002)

**INT-CL (IPC):** H04B007/26

**EUR-CL (EPC):** H04L012/28 , H04L029/06

**ABSTRACT:**

CHG DATE=20031203 STATUS=O>The present invention discloses an authentication system and method having mobility in a public wireless LAN. The authentication system includes an access point for requesting authentication of a wireless terminal to an access point manager, enabling data transmission and reception of the authenticated wireless terminal, and requesting the access point manager to charge the wireless terminal, and the access point manager for authenticating the wireless terminal which has already been authenticated on the basis of previously-registered registration information upon the request of the access point, authenticating the wireless terminal which has not been registered through an authentication server of a wireless network operator, and transmitting the authentication information to the access point. As a result, the wireless terminal can continuously access the network through the access points of the same subnet as well as different subnet without re-authentication, thereby achieving mobility and processing charging.